

REMARKS

Claims 1-3, 5-7 and 9-13 are pending. By this Amendment, claims 1, 3, 5-7 and 9-13 are amended. Claims 4 and 8 are canceled without prejudice or disclaimer. No new matter is introduced.

Applicant appreciates the courtesies extended to Applicant's representative, Mr. Paul Tsou, during the July 3 personal interview. The substance of the personal interview is incorporated in the remarks below.

The Office Action rejects claim 10 under 35 U.S.C. §112, first paragraph. Claim 10 is amended to obviate this rejection. Withdrawal of the rejection of claim 10 under 35 U.S.C. §112, first paragraph, is respectfully solicited.

The Office Action rejects claims 1-10 and 12 under 35 U.S.C. §102(b) over Subramaniam (U.S. Patent No. 6,081,900); and claims 11 and 13 under 35 U.S.C. §103 over Subramaniam. These rejections are moot with respect to canceled claims 4 and 8 and respectfully traversed with respect to the remaining claims.

The Office Action asserts that Subramaniam discloses all the subject matter recited in claims 1-10 and 12 and that the subject matter recited in claims 11 and 13 are obvious referring to the following portions of Subramaniam:

Col. 5, lines 44-49;

Col. 6;

Col. 8, lines 50-53; and

Col. 12, lines 40-46.

However, all of these references assume a network architecture as shown in Fig. 1 of Subramaniam, where an external client 112 communicates with various servers within secure network 100. Other clients 114 may communicate with secure network 100 via network 116 and client 112.

Throughout the Office Action, the assumption is made that the recited authentication server and the connection server are some combination of the target server 104 and the border server 106 in Subramaniam. However, Subramaniam does not contemplate the network association and authentication structure recited in the above claims and thus, Subramaniam is not relevant to any of the subject matter recited in claims 1-3, 5-7 and 9-13.

In particular, the Office Action asserts that Subramaniam discloses a retention unit for storing second connection authentication information generated based on first connection authentication information pointed to col. 6, line 52. There, Subramaniam discloses that the target server would generally check user permissions against access control lists associated with the data or take other steps to make sure that requesting user is entitled to access the request data before providing that data. As agreed to during the interview, Subramaniam does not disclose or suggest discloses a second connection authentication information generated based on first connection authentication information recited in claims 1 and 3, or storing encrypted user names and passwords, as recited in claims 6 and 7.

Additionally, the Office Action asserts that the redirector on border server 106 is the "second unit" recited in claims 1, 3, 6 and 7. Here, the Office Action appears to broadly assert that either border server 106 or target server 104 may be viewed as an authentication server. In either case, Subramaniam does not disclose or suggest that either border server 106 or target server 104 transmits a connection server address to the client apparatus, as recited in claim 1, 3, 6 and 7. Indeed, there is no need to do so since client 112 of Subramaniam already has the address for border server 106/target server 104.

Moreover, the Office Action asserts that border director 106 meets the "sixth unit" limitation recited in claim 1 citing C6/L61-64 of Subramaniam. However, here, Subramaniam discloses border server 106 redirecting client request to target server 104 and does not disclose or suggest "allowing the first connection authentication information to be

received from the client which is received from the authentication server." In fact, in the context of Subramaniam, such an operation appears unnecessary since border server 106 redirects client requests to target server 104. Border server 106 cannot be the recited connection server, since border server 106 does not receive connection authentication information from target server 104. Accordingly, Subramaniam does not disclose or suggest the subject matter recited in claims 1, 3, 6 and 7.

Regarding claim 5, the Office Action asserts that target server 104 is the connection server (unlike the Office Action assertion on page 5 that border server 106 is the connection server), pointing to C6/L44-49 of Subramaniam. Here, Subramaniam discloses that the target server 104 checks the IP address of the request. However, claim 5 recites that the connection server's control unit receives the client address after the authentication server authenticates information received from the client address. There is nothing in Subramaniam that discloses or suggests that border server 106 (now the authentication server) authenticates, but rather it redirects. Thus, target server 104 does not receive the client's address after client information is authenticated but rather the target server 104 appears to perform verification, i.e., checks the IP address. Thus, Subramaniam does not disclose or suggest the subject matter recited in claim 5.

Regarding claim 9, the Office Action asserts that Subramaniam discloses a retention unit that stores local authentication information pointing to C8/L50-53 disclosing that border server 106 receives user name and password. However, claim 9 recites that the local authentication information associates unique information of the client apparatus with a user name and a password. Subramaniam does not disclose or suggest anything regarding associating unique information of the client apparatus with user name and password. Thus, Subramaniam does not disclose or suggest the subject matter recited in claim 9.

Regarding claim 10, the Office Action cited C6/L42-48. However, Subramaniam does not disclose or suggest that the target server 104 allows communication from the address of the client apparatus for a predetermined period.

The Office Action cites col. 5, lines 44-49, against claims 12 and 13 asserting that Subramaniam discloses that servers 104 and 106 may be configured by those of skilled in the art in a wide variety of ways to operate as internet servers, proxy servers as directory service providers or name servers as software complements or other object servers or as a combination thereof. However, this passage does not disclose or suggest storing in/by the authentication server second connection authentication information required by the connection server based on the first connection authentication information, as recited in claims 12 and 13. There is nothing in Subramaniam that discloses this recited subject matter. While Subramaniam in this passage discloses a very broad array of possibilities, there is nothing enabled or explicitly disclosed that relates to the specific subject matter recited in claims 12 and 13.

Further, the Examiner cites col. 8, lines 50-53, to support the assertions that Subramaniam discloses transmitting by client apparatus the second connection authentication information to the received connection server address, as recited in claim 12 and similarly in claim 13. However, this portion of Subramaniam only discloses that the user name and password are then transmitted over the secure connection to the border server which passes them in turn to the authentication system within the secure network 100. There is nothing in Subramaniam disclosing that the authentication server receives the connection server address. Indeed, there is no reason to do so since, as assumed by the Office Action, the authentication server and the connection server are the very same server.

Regarding claim 11, the Office Action asserts that Subramaniam discloses at col. 12, lines 40-46, that the authentication information may include certificates, tokens, public keys,

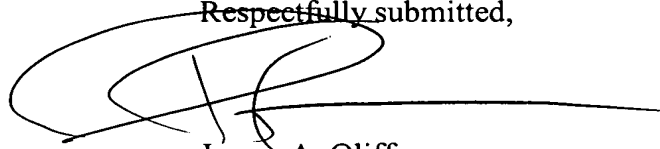
biometric scans, voice prints, retinal lens, etc. However, claim 11 recites that the client apparatus calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server, and acquires local authentication information associating the first authentication information with a predetermined second authentication information from the connection server to store the local authentication information. In other words, claim 11 requires a certain relationship between various types of authentication information and storing the different types of authentication information in different locations. There is nothing in Subramaniam that discloses such subject matter but merely that different types of information may be used as authentication information. Subramaniam is simply not directed to the same type of subject matter recited in claims 1, 3, 5-7 and 9-13. There is nothing in Subramaniam that discloses generating an authentication information based on other authentication information and storing different ones of the authentication information in different servers.

In view of the above, Subramaniam does not disclose or suggest the subject matter recited in claims 1, 3, 5 and 9-13 because a completely different network structural context is contemplated. Claim 2 depends from claim 1. Accordingly, Subramaniam does not disclose or suggest the subject matter recited in claims 1-3, 5-7 and 9-13. Withdrawal of the rejection of claims 1-13 under 35 U.S.C. §102(b) and §103 is respectfully solicited.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claims 1-3, 5-7 and 9-13 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'James A. Oliff', written over the words 'Respectfully submitted,'.

James A. Oliff
Registration No. 27,075

Paul Tsou
Registration No. 37,956

JAO:PT/eks

Date: July 3, 2007

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

<p>DEPOSIT ACCOUNT USE AUTHORIZATION Please grant any extension necessary for entry; Charge any fee due to our Deposit Account No. 15-0461</p>
